AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of

The residence at 1422 Wilson Avenue, Columbus, OH 43206, including the dwelling, curtilage, detached structures and any vehicles located therein

Case No. 2:21-mj-441

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property

The residence at 1422 Wilson Avenue, Columbus, OH 43206, including the dwelling, curtilage, detached structures and any vehicles located therein. (See Affidavit in Support of Application for a Warrant to Search and Seize)

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachement B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 USC 1344	Bank Fraud

The application is based on these facts:

As set forth in the attached Affidavit of Postal Inspector J. Michael McClelland

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

J. Michael McClelland, U.S. POSTAL INSPECTOR

Printed name and title

Sworn to before me and signed in my presence.

Date: June 25, 2021

City and state: COLUMBUS, OHIO

Kimberly A. Johnson
United States Magistrate Judge

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF: 1422 Wilson Avenue Columbus, OH 43206	**MISC NO.**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, Jan Michael McClelland, Postal Inspector, being duly sworn, depose and state as follows:

1. I make this affidavit in support of an application or a warrant to search the following premises:

a. 1422 Wilson Avenue, Columbus, OH 43206 (DAVID ROBINSON'S residence), hereinafter "PREMISES A," further described in Attachment A;

2. I have been a U.S. Postal Inspector with the U.S. Postal Inspection Service in Columbus, OH and have been so employed since March 2015. My responsibilities include investigating money laundering, financial crimes, identity theft, mail theft, mail fraud, bank fraud, intellectual property fraud, prohibited mailings, dangerous mail, and other violations with a nexus to the U.S. Postal Service (USPS). Prior to becoming a U.S. Postal Inspector, I was a Special Agent with the U.S. Secret Service from December 2002 through March 2015. My responsibilities as a Special Agent included investigating financial crimes, identity theft, counterfeit currency, bank fraud, wire fraud, access device fraud and threats against the President and Vice President.

INTRODUCTION

3. This affidavit is also based upon information that I have obtained from other law enforcement officers. This affidavit is intended to show only that there is sufficient probable

cause for the requested warrant and does not set forth all of my knowledge about this matter.

TECHNICAL TERMS

4. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

c. Portable media player: A portable media player is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store

very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

5. Based on my training, experience, and research, I know that wireless telephones have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and personal digital assistant, which stores names, addresses, appointments, and notes, among other information. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

6. Based on my training, experience, and research, I know that GPS navigation devices that determine location and assist in navigating to specific locations can uncover, among other things, evidence that reveals or suggest who possessed or used the device and information about specific locations that may be relevant in a criminal investigation.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

7. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other

storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

8. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

9. *Probable cause*. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

10. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

d. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

11. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of date recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Facts Supporting Finding of Probable Cause

13. On or about December 7, 2020, the Gahanna Division of Police (GDP) responded to Huntington National Bank (HNB), 380 S. Hamilton Road, Gahanna, OH on a report of fraudulent checks being passed. Victim D.H. reported that three (3) checks cleared her account that were fraudulent. The fraudulent checks had various names and addresses as the payee, but the bank account information returned to D.H. HNB account. One of the fraudulent checks was made payable to HomeGoods at 2000 Park Manor Blvd., Pittsburgh, PA.

14. On or about December 2020, the GDP received a second report, that a victim had a fraudulent check drawn on their HNB account that was made payable to HomeGoods. GDP obtained video surveillance from the HomeGoods store in Pittsburgh, PA of the above transaction involving a fraudulent check drawn on D.H. HNB account. HomeGoods investigators reported to GDP that as of December 14, 2020, they have received over $14,000 in fraudulent checks from stores located in Indiana, Ohio, Illinois and Kentucky.

15. On or about March 14, 2021, TJ Maxx Organized Retail Crime Investigator contacted the GDP regarding fraudulent activity at their businesses. TJ Maxx has identified approximately $291, 326 in loss as a result of purchases and returns made with fraudulent checks. TJ Maxx provided surveillance photographs and transactions of suspects making purchases with fraudulent checks at TJ Maxx, Marshall's, and HomeGoods stores.

16. The GDP was able to identify two (2) of the subjects in the surveillance photographs provided by TJ Maxx as David Lashawn Robinson and Leearl M. Chapman.

17. TJ Maxx Organized Crime Investigator provided copies of the fraudulent checks used to make purchases at their stores. TJ Maxx advised that clerks are required to ask for an official identification card, which is normally a driver's license, when a customer uses a personal

check for payment. TJ Maxx clerks are required to confirm that the name on the driver's license provided matches the name on the checks presented for payment. Several of the checks provided by TJ Maxx have an identification number written on the checks that was completed by the clerk at the store. This identification number reflects the number that was on the identification provided by the customer. Robinson is identified on video surveillance as providing numerous checks in different names that have identification numbers written on the checks. Database searches revealed that the identification numbers written on the fraudulent checks do not match the names and addresses that are on the checks.

18. David Robinson has an Ohio Driver's License that was issued on May 3, 2021, that reflects 1422 Wilson Avenue, Columbus, OH 43206 as his residence.

19. Surveillance at 1422 Wilson Avenue, Columbus, OH 43206, revealed two (2) vehicles registered to David Robinson parked in the driveway at the above address.

20. On or about June 17, 2021, law enforcement recovered the following items from the refuse that was placed at the curb of 1422 Wilson Avenue, Columbus, OH 43206:

a. Receipt for a purchase made at HomeGoods store in Richmond, KY on May 29, 2021.
b. Receipt for items returned to Marshall's store in Gahanna, OH on June 14, 2021. Several of the items returned were items that were purchased at the HomeGoods store in Richmond, KY on May 29, 2021.

21. TJ Maxx provided surveillance photographs of the suspect, identified as Robinson, purchasing the items on the above receipt at the HomeGoods store in Richmond, KY on May 29, 2021. In addition, TJ Maxx provided surveillance photographs of the suspect, identified as Robinson, returning items at the Marshalls store in Gahanna, OH on June 14, 2021.

22. Based upon my training and experience I know that individuals frequently carry cellular telephones with them. As such, I know that individuals conduct criminal activity such as bank fraud, often use multiple computers, cellular telephones and other media storage devices to conduct such fraud and communicate with others involved. In addition, I know that computers and electronics are used to create fraudulent identification cards.

23. Based on the foregoing, it is your affiant's contention that there is probable cause to believe that there is evidence related to criminal activity involving bank fraud, in violation of Title 18, United States Code, Section 1344, involving the user of the items listed in Attachment B.

Conclusion

24. Based on the facts set forth in this Affidavit, I maintain there is probable cause to believe that the requested information will lead to evidence regarding the activities described above. The requested information is necessary to determine other victims/suspects, victim/suspect information, and other suspect whereabouts.

25. Based on the facts set forth in this Affidavit, I maintain there is probable cause to believe that there is evidence regarding the activities described above, in violation of Title 18, United States Code, 1344, located in the items listed on Attachment A. The information is necessary to determine other victims/suspects, victim/suspect information, and other suspect information and whereabouts.

26. A description of the premises to be searched can be found in Attachment A. A description of the items to be searched and seized can be found in Attachment B.

27. Accordingly, I respectfully request that the Court issue a Search Warrant for 1422 Wilson Avenue, Columbus, OH 43206, including the dwelling, curtilage, detached structures and any vehicles located therein and seize the items described in Attachment B.

J. Michael McClelland
United States Postal Inspector

Sworn to before me, and subscribed in my presence, this 25th day of June 2021, in Columbus, Ohio.

Kimberly A. Johnson
United States Magistrate Judge

ATTACHMENT A

Premises A to be searched

The premise to be searched is located at 1422 Wilson Avenue, Columbus, OH 43206. It is a two story single family home, with white siding, with the number 1422 in black above the mail box near the front door. The garage is detached from the residence.

ATTACHMENT B

1. All records relating to violations involving bank fraud in violation of Title 18 United States Code, section 1344 and those violations involving DAVID LASHAWN ROBINSON AND LEEARL M. CHAPMAN:

a. All records and other documents related to fraudulent activity involving bank fraud, identity theft and fraudulent identification.

b. Log books, records, payment receipts, notes, and/or customer lists, ledgers and other papers relating to transportation, ordering, purchasing, processing, storage, and distribution of personally identifiable information, in particular IDs and checks;

c. types, amounts, and prices of credit/debit/gift cards, as well as dates, places, and amounts of specific transactions, and travel records. Evidence of such travel is often times maintained by individual's conducting bank fraud in the form of airline receipts, bus tickets, auto rental receipts, credit card receipts, travel schedules, diaries, hotel receipts, logs, travel agency vouchers, notes, cellular telephone tolls, and records of long-distance telephone calls;

d. any information related to sources of victims personal identifying information (including names, addresses, phone numbers, or any other identifying information);

e. Photographs, including still photos, digital images, negatives, video tapes, digital videos, films, undeveloped film and the contents therein, slides, in particular, photographs of co-conspirators, of assets and/or criminal activity.

f. Address and/or telephone books, rolodex indices, and any papers reflecting names, addresses, telephone numbers, pager numbers, fax numbers of co-conspirators, sources of supply, storage facilities, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists.

g. The opening and search, and removal, if necessary, of any safe or locked receptacle or compartment, as some or all of the property heretofore may be maintained.

h. all bank records, storage unit records, safe deposit box records, stored value cards, credit cards, checks, credit card bills, account information, and other financial records.

i. Electronic equipment, such as, computers, external electronic storage media (such as external hard drives and computer disks) and other associated equipment and accessories necessary to examine and record data stored in said computers and storage media (such as monitors, printers, external drives, and other peripherals).

In the event that the agents cannot obtain access to any subject computer or cannot search for or copy information contained on that computer, the agents are

then authorized to seize such computer and remove it to a laboratory setting for a sufficient period of time to obtain access to, search for, and recover the files and records described herein. Such computer may be "imaged." An image is a pristine, bit-by-bit reproduction of the subject's computer hard drive. In addition, if the files and records cannot be read and understood without the software or programs that created those files or records, the agents are authorized to seize such software and any documentation and manuals that describe the software and give instructions on its installation and use.

j. All cellular and "smart" telephones to include their SIM cards, all related documentation and all stored data to include passwords, encryption keys, access codes, SIM passwords, files, programs, ring tones, pictures, videos, phone books, call history, voice mail, e-mail, text messages, deleted messages audio and/or text and geographical information, and proof of ownership to include correspondence, registration keys or similar items and all cellular related accessories not specifically mentioned herein. To be able to download/retrieve all information from the cellular telephone and put all data into human readable form.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.